SUPPORT de COURS

Thierry DESPRATS

II - La COUCHE RESEAU dans le modèle TCP/IP

Sommaire

ADRESSAGE IP (1/6) : PRINCIPES

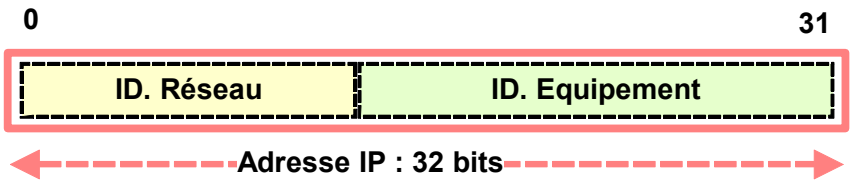
- **PRINCIPE de BASE :**
  - **Identification universelle des équipements**
  - **Méthode analogue à celle de l'adressage physique :**

> ***« Chaque équipement reçoit une adresse binaire unique sur 32 bits »***

= = > « ADRESSE INTERNET » ou « ADRESSE IP »

- **FORMAT de BASE des ADRESSES IP :**
  - **Concaténation de :**
    - **Un identifiant de réseau (@sse réseau)**

    et de :
    - **Un identifiant d'équipement (@sse équipement)**



  - **Longueur de chaque partie dépend de la classe d'adressage**
  - **Utilité pour la fonction de routage**

    = = > ***« Les adresses IP des équipements connectés à un même réseau ont toutes un préfixe commun (ID réseau).»***

- **PLUS PRÉCISÉMENT … :**
  - **ADRESSE IP < = = = > POINT d'ACCÈS à un RÉSEAU :**

L'adresse IP attribuée à un équipement désigne à la fois un réseau et cet équipement sur ce réseau, donc un point d'accès à un réseau pour un équipement.

ADRESSAGE IP (2/6) : les CLASSES

- **OBJECTIF et PRINCIPE :**

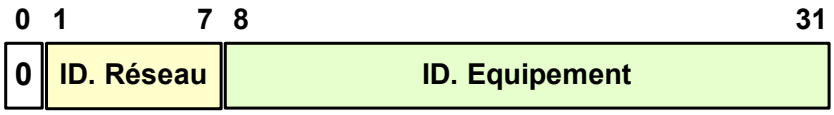
  ☞ ***Adapter l'adressage aux différentes tailles des réseaux :*** ***l'appartenance à une classe fixe le format de la construction d'une adresse IP (longueur des parties @sse réseau et @sse équipement).***

  ☞***Favoriser une interconnexion hiérarchisée***

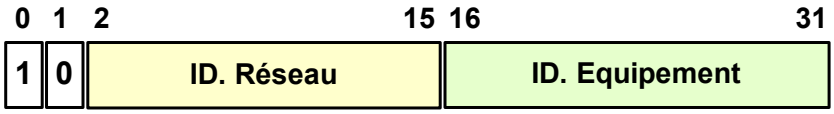
  ☞***Les premiers bits de forts poids déterminent la classe d'une @sse***

- **Les 5 CLASSES :**

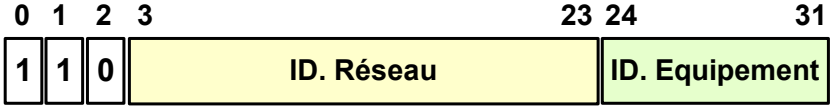
  - **CLASSE A** : ***réseaux de plus de 65.536 équipements connectés***



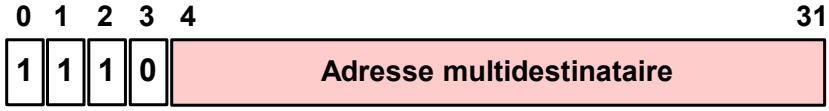
  - **CLASSE B** : ***réseaux qui ont entre 256 et 65.536 équipements***



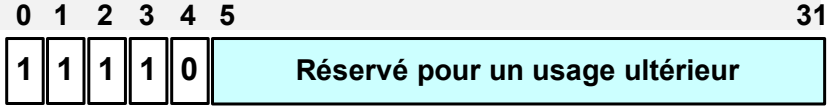
  - **CLASSE C** : ***réseaux qui moins de 256 équipements connectés***



  - **CLASSE D** : ***diffusion multidestinataire (IGMP).***



  - **CLASSE E :**



ADRESSAGE IP (3/6) : NOTATION DÉCIMALE POINTÉE

- **OBJECTIF :**

  Mettre à disposition des administrateurs, des programmeurs et des utilisateurs une notation des adresses IP plus aisée à manipuler qu'une suite de 32 bits…

- **PRINCIPE :**

  Exprimer la valeur binaire de chacun des 4 octets d'une adresse en sa valeur décimale équivalente,

  Séparer par un point les quatre valeurs décimales ainsi obtenues.

- **EXEMPLES :**

  - Soit l'adresse IP représentée en binaire :

  10000000 00001010 00000010 00011110

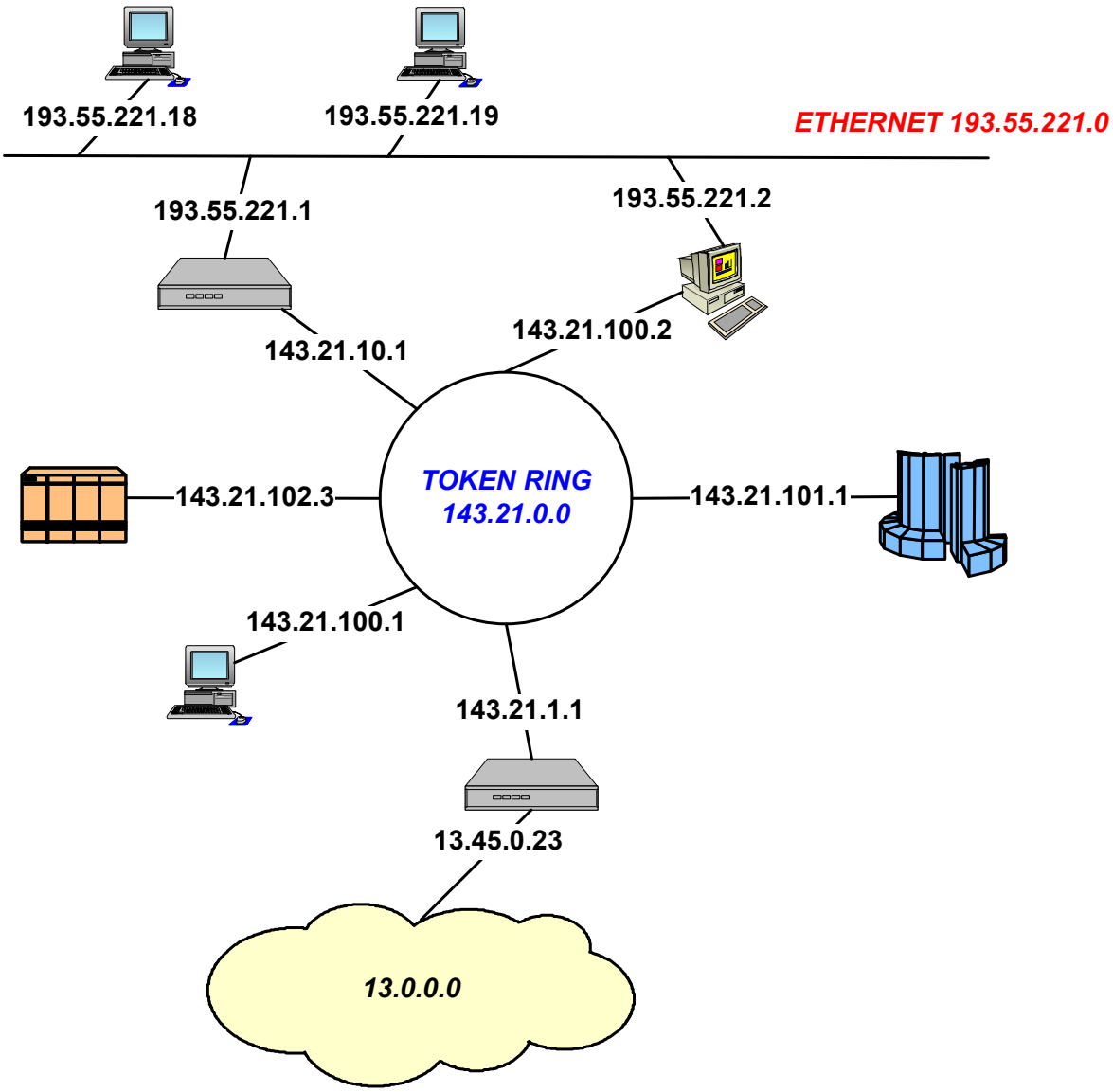
  La notation décimale pointée équivalente est : **128.10.2.30**

  - De la même façon :

  11111111 11111111 11111111 11111111

  s'exprime par : **255.255.255.255**

ADRESSAGE IP (4/6) : EXEMPLE



ADRESSAGE IP (5/6) : ADRESSES PARTICULIÈRES

- **ADRESSES de DÉSIGNATION :**

  Elles ne sont jamais attribuées à des équipements

  Elles sont utilisées soit :

  - ***comme « adresse source » lors d'un envoi de datagramme lors d'opérations de démarrage,***
  - ***pour désigner des réseaux dans des tables de routage.***

  La valeur « tout à zero » permet de désigner « cet » objet

Valeur d'adresse		*Signification*	*Exemple*
Tout à zéro		*«Cet» équipement*	0.0.0.0.
ID_Réseau	Tout à zéro	*«Ce» réseau*	193.55.221.0

- **ADRESSES de DIFFUSION :**

  Elles ne sont jamais attribuées à des équipements

  Elles sont utilisées comme « adresse destination » lors d'un envoi de datagramme destiné à être diffusé.

  La valeur « tout à un » permet de désigner « tous » les objets

Valeur d'adresse		*Signification*	*Exemple*
Tout à un		*Diffusion limitée*	255.255.255.255
ID_Réseau	Tout à un	*Diffusion dirigée*	193.55.221.255

- **ADRESSE de REBOUCLAGE (loopback) :**

  Adresse 127 de la classe A dédiée à la « simulation » d'un réseau.

  Utilisée pour des communications locales ou des tests : non routée.

  Tout host à une interface sur ce réseau (ex : **127.0.0.1***)*

ADRESSAGE IP (6/6) : MISE en PLACE

- **ADRESSES OFFICIELLES routables sur INTERNET :**

  ☞ ***L'IANA (Internet Assigned Number Authority) est l'organisme officiel qui gère les identificateurs et fixe la politique d'affectation dans l'Internet : il est le garant de l'unicité des « adresses réseaux » attribués aux réseaux constituant l'Internet.***

  ☞ ***Toute organisation qui souhaite mettre en place un internet connecté à l'Internet, doit s'adresser aux délégations nationales de l'IANA. (Pour la France, il s'agit de NIC-France hébergé à l'INRIA).***

  ☞***Cet organisme national assigne alors à l'organisation uniquement un identificateur de réseau (ou plage d'adresses). Celui-ci appartient à une classe qui correspond à la taille pressentie du réseau.***

  ☞***L'organisation met ensuite en place son propre plan d'adressage (schéma d'affectation d'adresses IP aux équipements) et prend soin de faire débuter toutes les adresses par le préfixe assigné.***

- **ADRESSES PRIVÉES :**

  ☞***Mettre en place son propre plan d'adressage IP en prenant des valeurs correctes au sens du format MAIS qui n'ont aucune réalité dans une interconnexion avec le réseau Internet :***

  = = > interconnexion « brute » IMPOSSIBLE avec l'Internet

  = = > utilisation de NAT (Network Address Translation)

  ☞ ***Classe A : 10.*.*.****

  Classe B : 172.16.*.* à 172.31.*.*

  Classe C : 192.168.0.* à 192.168.255.*

- **TECHNIQUES d' ATTRIBUTION d'une ADRESSE IP :**

  ☞***de façon manuelle et statique par l'administrateur :***

  commandes : ifconfig, ipconfig….

  ☞***de façon automatique et statique :***

  protocoles RARP, BOOTP

  ☞***de façon automatique et dynamique :***

  protocole DHCP

SOUS-ADRESSAGE IP (1/2) : PRINCIPE

- **OBJECTIFS :**

  - ***Limiter la consommation d'adresses IP (saturation des classes B et C)***

  - ***Faciliter l'administration des réseaux d'entreprise (généralement plusieurs sous-réseaux interconnectés)***

- **PRINCIPE :**

  Extension standardisée de l'adressage IP : Réserver dans la partie locale d'une adresse IP (partie adresse d'équipement) un certain nombre de bits pour coder des adresses de sous-réseaux « locaux ».

Adressage d'un sous-réseau		
ID réseau	***ID ss-réseau***	***ID équipement***
Préfixe Internet	**Adressage local**	

= = > hiérarchisation du réseau global IP en sous-réseaux IP

= = > transparence assurée de l'extérieur (le préfixe Internet reste inchangé)

= = > routage optimisé à l'intérieur

- **NOTION de MASQUE de SOUS-RÉSEAUX :**

  Masque de sous-réseaux : information nécessaire aux équipements du réseau IP lors de l'analyse d'une adresse IP pour déterminer les longueurs des différentes parties.

Codage à 1 de la partie adresse de sous-réseau		
Tout à 1	***Tout à 1***	***Tout à 0***

= = > utilisation dans tout le réseau pour un routage cohérent

= = > masque présent dans les tables de routage

SOUS-ADRESSAGE IP (2/2) : ILLUSTRATION

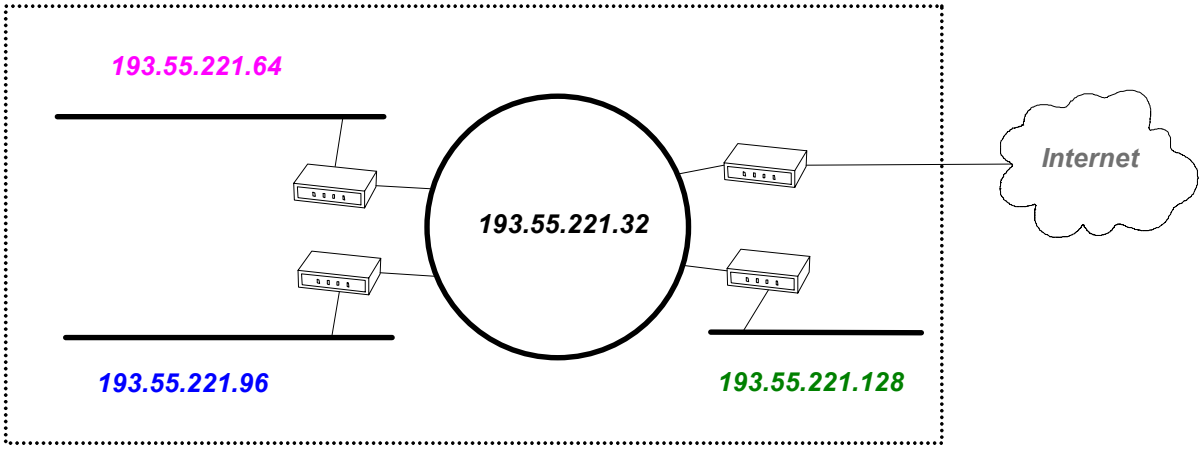
- **EXEMPLE de SOUS-ADRESSAGE :**

Sous-adressage sur 3 bits d'un réseau de classe C :

- ***Adresse de classe C :*** `193.55.221.0`
- ***4 sous-réseaux déterminés (d'au plus 30 éqts)***
- ***valeur du masque de sous-réseau :***
- ***en binaire :*** `11111111 11111111 11111111 11100000`
- ***notation décimale pointée :*** `255.255.255.224`
- ***autre notation :*** `193.55.221.0/27`

- **APPLICATION :**

Décomposition du réseau `193.55.221.0` ***:***



IP (1/9) : CARACTÉRISTIQUES GÉNÉRALES

Un internet < = = > un réseau virtuel :

IP favorise l'abstraction des réseaux réels en offrant des fonctions de transmission de données structurées en bloc, les datagrammes, sur ces réseaux = => Couche 3

Les services de plus haut niveau apportent à l'utilisateur une valeur fonctionnelle plus riche.

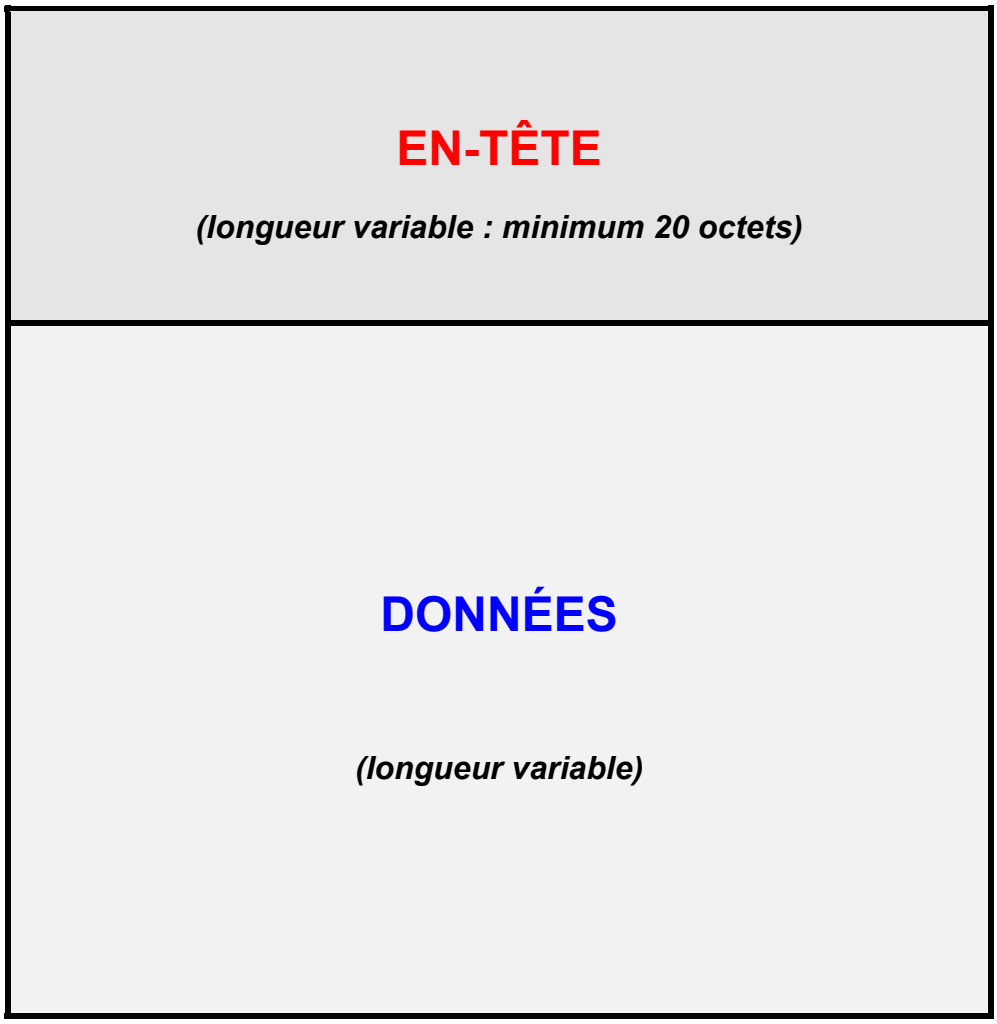
- **CARACTÉRISTIQUES du SERVICE IP :**
  - ***Mode non connecté***
    - ☞*Une phase unique de transfert de données*
    - ☞ *Chaque datagramme est traité indépendamment des autres (paradigme de « remise au mieux », « best effort delivery »)*
  - ***Non fiable, sans garantie de remise***
    - ☞*Perte, duplication, retard, altération, déséquencement possibles*
    - ☞*De façon brute, IP ne détecte pas ces problèmes, et ne prévient ni l'émetteur, ni le destinataire de leurs occurrences.*

- **CARACTÉRISTIQUES du PROTOCOLE IP :**
  - ***PDU = datagramme***
    - ☞*Un datagramme : unité de donnée de base circulant sur un internet.*
    - ☞*Son en-tête contient les informations nécessaires à la réalisation du protocole.*
  - ***Fonction de routage***
    - ☞*Déterminer le chemin le long duquel les datagrammes transitent.*
  - ***Règles opérationnelles***
    - ☞*Comment un équipement terminal (Host), un routeur (Gateway) doit traiter les datagrammes (fragmentation/réassemblage, destruction…)*

IP (2/9) : FORMAT d'un DATAGRAMME IP

IP : ***Internet Protocol*** ***(RFCs 791 – 760)***

DEUX PARTIES :

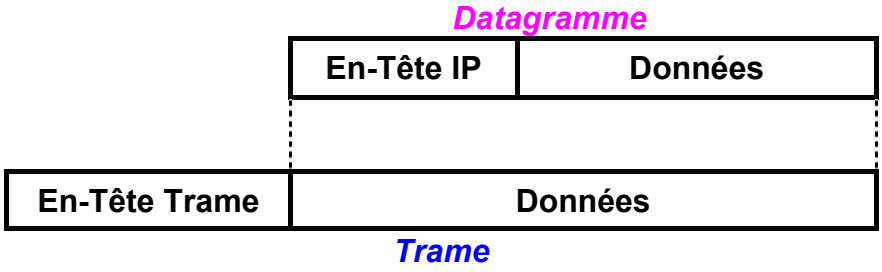


TAILLE MAXIMALE :

2^{16} = = > 64 k octets

IP (3/9) : ENCAPSULATION des DATAGRAMMES

- **ENCAPSULATION dans les TRAMES de LIAISON :**



Quelle taille générale choisir pour un datagramme ?

- **NOTION de MTU :**

MTU : Maximum Transfer Unit

> ***"Valeur en octets de la taille maximale du champ de données d'une trame"***

Déterminée officiellement pour chaque standard

Liée aux caractéristiques technologiques d'un type de liaison :

- ***débit***
- ***fiabilité***

= = > *Pas de taille idéale des datagrammes*

= = > *Nécessité pour IP d'adapter cette taille*

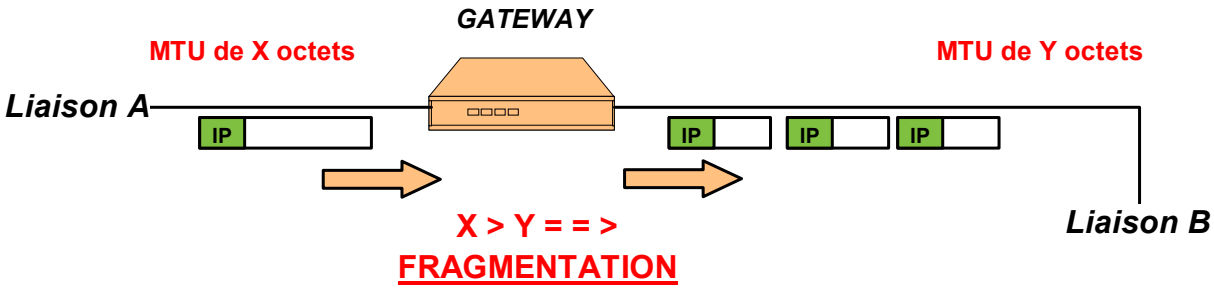
= = > *FRAGMENTATION NECESSAIRE*

= = > *RÉASSEMBLAGE NECESSAIRE*

IP (4/9) : FRAGMENTATION/RÉASSEMBLAGE

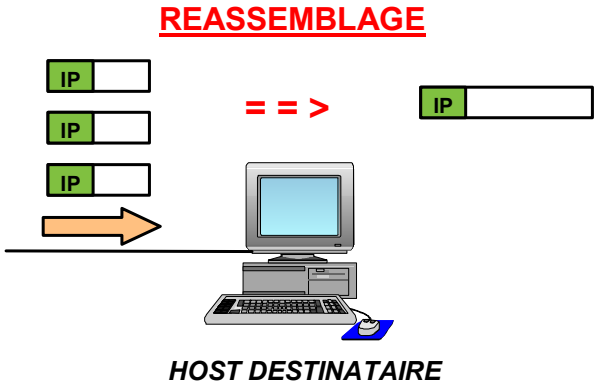
- **OPÉRATION de FRAGMENTATION :**

SEULS, les ROUTEURS peuvent être amenés à FRAGMENTER :



- **OPÉRATION de RÉASSEMBLAGE :**

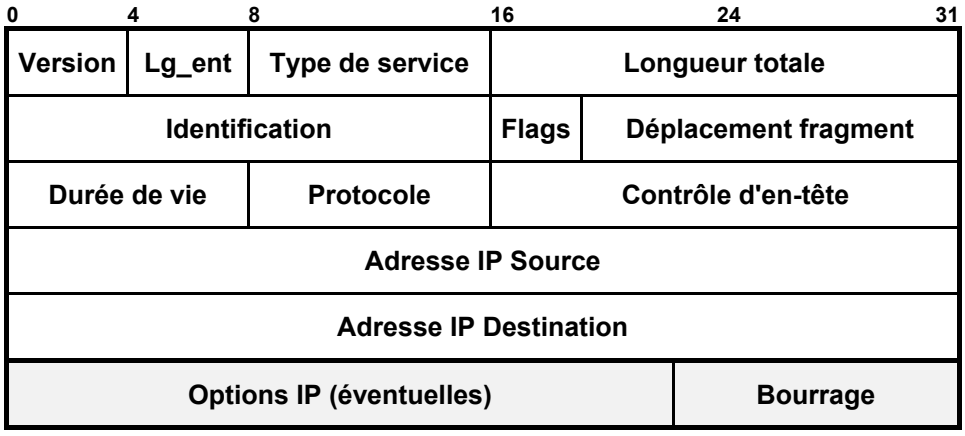
SEUL, l'équipement DESTINATAIRE est habilité à RÉASSEMBLER les fragments d'un datagramme initial :



= = > Nécessité de GERER LA FRAGMENTATION dans IP

IP (5/9) : FORMAT de l'EN-TÊTE (1/5)

- **STRUCTURE de l'EN-TÊTE IP :** **(RFCs 791 – 760)**



- **Champ VERSION :** ***(4 bits)***

Numéro de version du protocole IP utilisé pour créer le datagramme.

☞Permet à l'émetteur, aux routeurs et au destinataire de s'accorder sur le format.

☞Un équipement rejette un datagramme si sa version du logiciel IP ne correspond pas à celle indiquée dans ce champ.

- **Champ LG-ENT :** ***(4 bits)***

Longueur de l'en-tête exprimée en multiple de mots de 4 octets.

☞Si l'en-tête n'a pas d'options, la valeur de ce champ est 5 (20 Ø).

- **Champ LONGUEUR TOTALE :** ***(16 bits)***

Longueur totale du datagramme (en-tête + données) exprimée en nombre d'octets (au plus 65536).

☞D'où : Longueur données = Longueur totale – Longueur en-tête

IP (6/9) : FORMAT de l'EN-TÊTE (2/5)

- **Champ TYPE de SERVICE (ToS) :** *(8 bits)*

Façon dont le datagramme doit être géré (QoS).

0	1	2	3	4	5	6	7
Priorité			D	T	R	C	0

- **Champ PRIORITÉ :** *(3 bits)*

☞ *Degré de priorité du datagramme (peu utilisé, mais exploitation possible pour contrôle de congestion).*

☞*De* **0** *(priorité normale) à* **7** *(priorité forte – supervision)*

- **Bits D, T, R et C :** *(4 bits)*

☞ *Bit* **D** **(Delay)** *à 1 pour souhaiter un court délai d'acheminement du datagramme*

☞*Bit* **T** **(Throughput)** *à 1 pour souhaiter un fort débit pour la transmission du datagramme*

☞*Bit* **R** **(Reliability)** *à 1 pour souhaiter un fort degré de fiabilité de la transmission du datagramme*

☞*Bit C* **(Cost)** *à 1 pour souhaiter les coûts les plus faibles*

Uniquement des souhaits ! (pris en compte si routage le permet)

Exemples :		
	0 0 1 0	*Transfert de données*
	1 0 0 0	*Transfert de voix*
	0 1 0 0	*Transfert d'images.*

- **Champ IDENTIFICATION :** *(16 bits)*

Numéro unique attribué par l'émetteur (donc associé à l'adresse IP de la source) pour identifier le datagramme.

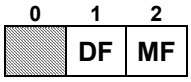
☞*Chaque source gère un compteur incrémenté à chaque émission.*

☞*Les fragments d'un même datagramme initial ont la même valeur d'identifiant : ce champ est utile au récepteur lors de l'opération de réassemblage pour déterminer l'appartenance à un datagramme initial.*

IP (7/9) : FORMAT de l'EN-TÊTE (3/5)

- **Champ FLAGS :** *(3 bits)*

  Contrôle de la fragmentation.



  - **Bit DF (Don't Fragment) :**

    ☞ ***Positionné à 1 pour interdire la fragmentation (cas spécifiques)***

    ☞***Si impossibilité, le datagramme est détruit***

  - **Bit MF (More Fragments) :**

    ☞***Indique que les données du datagramme sont les dernières du datagramme initial (valeur 0) ou pas (valeur 1).***

    ☞***Utilisé lors de l'opération de réassemblage***

Résumé :	**1 0**	***Fragmentation interdite***
	0 1	***Un fragment au milieu***
	0 0	***Le fragment de fin***

- **Champ DÉPLACEMENT FRAGMENT :** *(13 bits)*

  Indique la localisation des données transportées par le datagramme fragment par rapport au datagramme initial. Ce déplacement est exprimé en multiple de 8 octets, unité de fragmentation.

  ☞***Vaut 0 s'il s'agit d'un datagramme non fragmenté (bit MF à 0) ou s'il s'agit du premier fragment (bit MF à 1) d'un datagramme initial.***

  ☞***Utile au réassemblage, notamment pour déterminer l'ordre et le nombre des fragments.***

- **Champ DURÉE de VIE :** *(8 bits)*

  Durée maximum de transit du datagramme dans un internet : éviter les datagrammes qui bouclent …

  ☞***Chaque routeur diminue cette valeur : si elle devient nulle, il détruit le datagramme.***

IP (8/9) : FORMAT de l'EN-TÊTE (4/5)

- **Champ PROTOCOLE :** *(8 bits)*

  Numéro officiel du protocole de niveau supérieur qui a créé le message transporté par le datagramme dans sa partie données.

  ☞*Utile au récepteur pour déterminer à quel protocole de haut niveau sont adressées les données (RFC 1700) :*

TCP	*6*
UDP	*17*
ICMP	*1*
IGMP	*2*
OSPF	*89*
...	

- **Champ CONTRÔLE d'EN-TÊTE :** *(16 bits)*

  Checksum portant uniquement sur l'en-tête d'un datagramme.

  ☞*Utile aux routeurs lors de la modification d'en-tête dans le cas de fragmentation.*

  ☞*Complément à 1 de la somme complémentée à 1 des mots de 16 bits de l'en-tête du datagramme.*

  ☞*Si valeur incorrecte, le datagramme est détruit.*

- **Champ ADRESSE IP SOURCE :** *(32 bits)*

  Adresse IP de la source du datagramme.

  ☞*Adresse de désignation ou de rebouclage possible.*

- **Champ ADRESSE IP DESTINATION :** *(32 bits)*

  Adresse IP du destinataire du datagramme.

  ☞*Adresse de diffusion ou de rebouclage possible.*

IP (9/9) : FORMAT de l'EN-TÊTE (5/5)

- **Champ OPTIONS :** ***(longueur variable)***

Non obligatoire : tests, mises au point, supervision…

☞Plusieurs options peuvent se suivre (pas de séparateurs).

☞Trois principales catégories d'options définies :

- **Option "Enregistrement de route" :**

☞Chaque routeur rencontré sur le chemin du datagramme est invité à ajouter son adresse IP dans une liste initialement vide.

☞Le destinataire peut ainsi grâce à cette option récupérer la route empruntée par le datagramme depuis la source.

- **Option "Routage par la source" :**

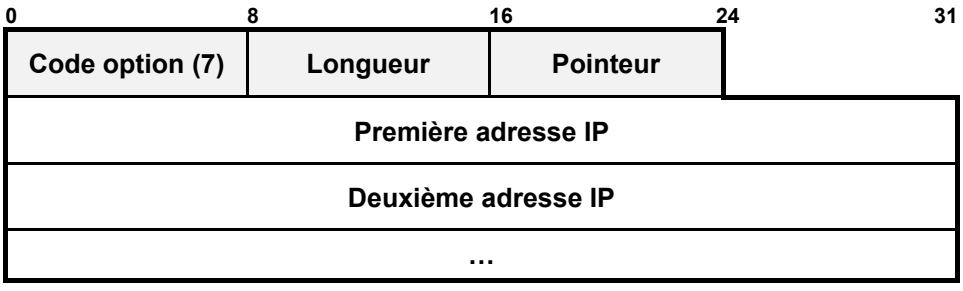
☞La source impose dans cette option une liste d'adresses IP des routeurs appartenant à la route que doit emprunter ce datagramme.

☞Possibilité de routage strict (code = 137) ou lâche (= 131).

- **Option "Horodatage" :**

☞Chaque routeur rencontré sur le chemin du datagramme est invité à indiquer la date et l'heure à laquelle il a traité ce datagramme (on peut lui demander éventuellement de préciser aussi son adresse IP).

Exemple de format : "enregistrement de route"



- **Champ BOURRAGE :** ***(longueur variable)***

Insertion d'autant de bits à 0 que nécessaire pour obtenir une longueur de datagramme multiple de mots de 32 bits (code option = 1).

ICMP (1/5) : OBJECTIFS

- **PROBLÈMES de NON REMISE de DATAGRAMMES :**
  - **Panne de liaisons**
  - **Panne de processeur**
  - **Destinataire physiquement déconnecté** ***(de façon temporaire ou permanente)***
  - **Expiration de la durée de vie d'un datagramme**
  - **Routeur en état de congestion** ***(impossibilité de traiter les messages entrants)***
  - **…**

= = > *QUI prévenir ?*

OBLIGATOIREMENT l'EXPEDITEUR

= = > *COMMENT le prévenir ?*

ENVOI d'un MESSAGE

= = > *QUE lui dire ?*

CAUSE du PROBLÈME et de l'envoi du MESSAGE

- **SUPERVISION du FONCTIONNEMENT de IP :**
  - **Tests d'accessibilité, contrôle de flux, demande d'informations…**

= = >Nécessité d'un mécanisme utilisé par les équipements pour s'échanger des informations de supervision et relatives aux erreurs

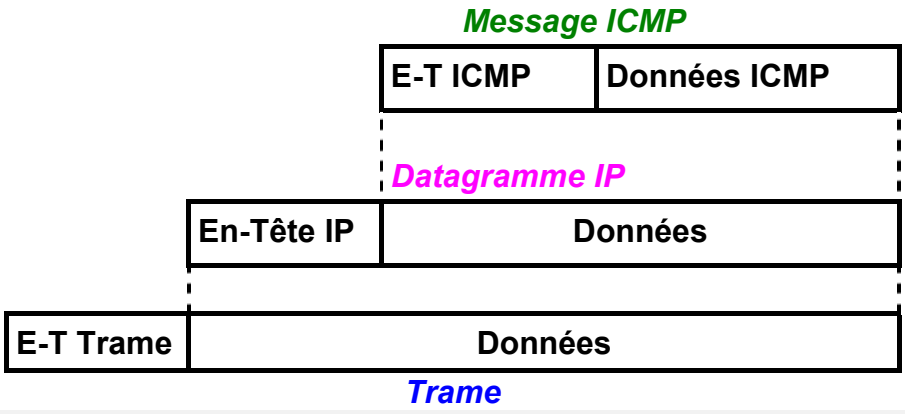
= = > PROTOCOLE ICMP

ICMP (2/5) : GÉNÉRALITÉS

ICMP : ***Internet Control and error Message Protocol*** ***(RFCs 792 – 777)***

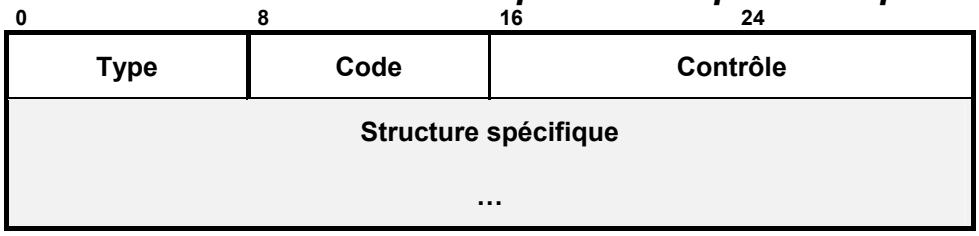
- **CARACTÉRISTIQUES GÉNÉRALES :**
  - ***ICMP est un module obligatoire qui doit être présent dans toute mise en œuvre de IP,***
  - ***Il permet de communiquer des messages d'erreur ou de supervision entre le logiciel IP d'un équipement et celui d'un autre équipement,***
  - ***ICMP ne réalise qu'une fonction de compte rendu d'erreur à l'expéditeur du datagramme non remis (pas de correction),***
  - ***Si ICMP détermine qu'un protocole de haut niveau est concerné, il en informe le module correspondant à ce protocole.***

- **REMISE des MESSAGES ICMP :**
  - ***Les messages ICMP sont acheminés par des datagrammes IP classiques (pas de priorité), numéro de protocole = 1.***
  - ***Ils sont soumis à des pertes, des destructions …***
    = = > pas de message ICMP généré dans ces cas (sinon congestion assurée…)



ICMP (3/5) : FORMAT et TYPES des MESSAGES

- **FORMAT des MESSAGES ICMP :**
  - ***Chaque type de message ICMP a son propre format ,MAIS, chacun d'eux commencent par 3 champs identiques :***



- **Champ TYPE :** ***(8 bits)***

  ☞***Définit la signification et le format du message ICMP.***

  ☞***Exemples de valeurs :***

Champ Type	*Signification du message ICMP*
0	Réponse à une demande d'écho
3	Destination inaccessible
4	Limitation de production à la source. Obsolète
5	Redirection (changement de route)
8	Demande d'écho
11	Expiration de délai pour un datagramme
12	Problème de paramètre d'un datagramme
13	Demande d'horodatage
14	Réponse à une demande d'horodatage
17	Demande de Netmask
18	Réponse à une demande de Netmask

- **Champ CODE :** ***(3 bits)***

  ☞***Raffinage du type du message.***

- **Champ TOTAL CONTRÔLE :** ***(16 bits)***

  ☞***Contrôle ne portant que sur le message ICMP (idem IP).***

- **PRINCIPALES CATÉGORIES de MESSAGES ICMP :**
  - ***Accessibilité (écho, inaccessibilité),***
  - ***Congestion et contrôle de flux,***
  - ***Problèmes de paramètres,***
  - ***Synchronisation d'horloges…***

ICMP (4/5) : MESSAGES d'ACCESSIBILITÉ

- **MESSAGES d'ÉCHO (*Ping*) :**
  - ***Permettent de tester l'accessibilité et l'état d'un équipement distant = = > connectivité au niveau IP***

0	8	16	24
Type (8 ou 0)	Code (0)	Total de contrôle	
Identificateur		Numéro de séquence	
Données optionnelles			
…			

  - **Champ DONNÉES OPTIONNNELLES :** ***(variable)***

    ☞***Données éventuellement précisées par l'expéditeur dans la demande et qui doivent lui être intégralement retournées dans la réponse émise par le destinataire.***

  - **Champs IDENTIFICATEUR et N° de SEQUENCE :** ***(32 bits)***

    ☞***Permettent à l'expéditeur d'associer les réponses reçues à ses propres demandes.***

- **COMPTE RENDU de DESTINATION INACCESSIBLE :**
  - ***Permet à un routeur qui ne peut délivrer un datagramme d'en informer l'expéditeur,***

0	8	16	24
Type (3)	Code (0-12)	Total de contrôle	
Inutilisé (à zéro)			
En tête + les 64 premiers bits du datagramme IP non remis			
…			

  - **Champ CODE :**

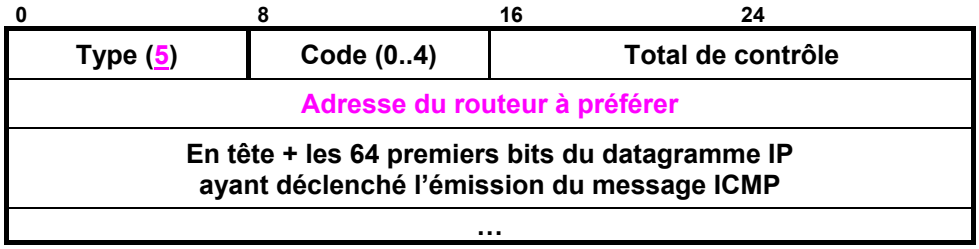
    ☞***Précise la raison de la non délivrance :***

0	Réseau inaccessible	7	Equipement destinataire inconnu
1	Equipement inaccessible	8	Equipement source isolé
2	Protocole inaccessible	9	Communication avec le réseau destinataire interdite
3	Port inaccessible	10	Communication avec l'équipement destinataire interdite
4	DF à 1 et Fragmentation nécessaire	11	Réseau inaccessible pour le service demandé
5	Echec de routage source	12	Equipement inaccessible pour le service demandé
6	Réseau de destination inconnu		

  - ***A l'aide de la partie du datagramme contenue dans le message ICMP, la source connaît l'adresse inaccessible.***

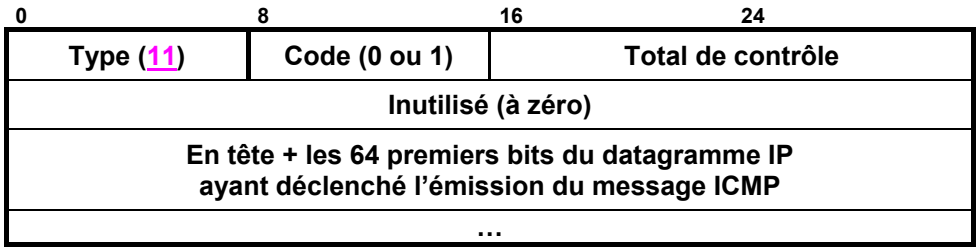
ICMP (5/5) : REDIRECTION et EXPIRATION de DÉLAIS

- **MESSAGE d'Indication de REDIRECTION :**
  - ***Permet à un routeur d'informer l'émetteur d'un meilleur routage pour atteindre la destination (station, (ss)réseau).***



  - ***A l'aide de la partie du datagramme contenue dans le message ICMP, la source peut modifier sa table de routage.***
  - ***Davantage utile aux stations…***

- **MESSAGE de DÉTECTION d'EXPIRATION de DÉLAIS :**
  - ***Permet à un routeur qui doit détruire un datagramme dont le champ "Durée de vie" (TTL) devient nul d'en informer l'expéditeur (Code 0).***
  - ***Permet à un host destinataire de prévenir que le délai de réssemblage a expiré et qu'il n'a pas reçu tous les fragments d'un datagramme initial. (Code 1).***



  - ***A l'aide de la partie du datagramme contenue dans le message ICMP, la source connaît le datagramme détruit et l'adresse du destinataire concerné par la non remise.***

ROUTAGE IP (1/7) : INTRODUCTION

ROUTAGE IP : ***déterminer dans un internet le chemin le long duquel les datagrammes sont transmis de l'équipement source jusqu'à la cible.***

Deux types d'équipements dans un internet :

- ***les hosts : équipements terminaux n'appartenant qu'à un seul réseau.***
- ***les routeurs : équipements reliés à au moins deux réseaux.***

= = > Hosts et routeurs participent au routage des datagrammes.

- **REMISE DIRECTE vs REMISE INDIRECTE :**

  - **La remise directe de datagramme :**

☞***Permet le transfert direct d'un datagramme entre deux équipements appartenant à un même réseau (même liaison).***

☞***Principe : l'expéditeur encapsule le datagramme dans une trame, effectue la correspondance (@sse IP, @sse physique) du destinataire, puis lui envoie directement la trame.***

☞***Cas d'utilisation : lorsque les préfixes des adresses IP de la source et de la cible sont identiques…***

  - **La remise indirecte de datagramme :**

☞***Le datagramme doit transiter par au moins un routeur pour atteindre un réseau autre que celui de l'expéditeur. Il transite de routeurs en routeurs jusqu'à ce que l'un d'entre eux puisse le remettre directement au destinataire.***

☞***Principe : l'expéditeur doit identifier au moins un routeur vers lequel envoyer le datagramme, puis lui faire parvenir (procédure semblable à la remise directe) celui-ci.***

☞***Cas d'utilisation : lorsque les préfixes des adresses IP de la source et de la cible diffèrent…***

= = > Nécessité de TABLES de ROUTAGE IP

- ne contenant que des adresses IP
- les plus réduites possibles
- suffisantes pour prendre des décisions de routage

= = >Plusieurs techniques :

ROUTAGE IP (2/7) : TABLES (1/1)

- **FORMAT des entrées dans les TABLES de ROUTAGE :**

Objectif :

☞*Exprimer l'information nécessaire à la phase de prise de décision de routage.*

Principe :

☞*Généralement, les entrées de la table de routage d'un équipement courant sont de la forme :*

(@sse IP de réseau, @sse IP d'équipement, *interface*)

où :

@sse IP de réseau : est celle de désignation d'un réseau destinataire.

@sse IP d'équipement : est celle d'un équipement « conduisant », directement ou non, au réseau dont l'adresse est @sse IP de réseau .

interface : représente l'interface de l'équipement courant sur la liaison à emprunter pour acheminer un datagramme vers l'équipement dont l'adresse est @sse IP d'équipement.

☞ *Il est également possible de travailler sur des adresses IP d'équipements (route de host à host) et non de réseau… essentiellement mises au point et tests.*

ROUTAGE IP (3/7) : TECHNIQUES (1/3)

- **EXPRESSION des CAS de « REMISE DIRECTE » :**

Principe :

☞***Dans ce cas :***

@sse IP de réseau : est la désignation d'un réseau destinataire sur lequel l'équipement possède l'interface interface.

@sse IP d'équipement : est l'adresse IP associée à l'interface interface de l'équipement sur ce réseau destinataire.

☞***Les préfixes des deux adresses mentionnées sont identiques.***

Illustration :

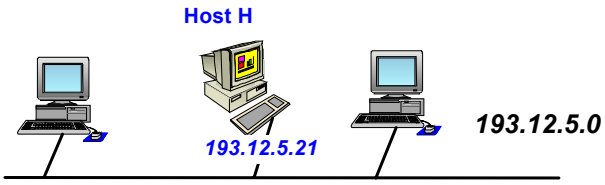


Table de routage de H (cas de remise directe)

Réseau destinataire	*Décision routage*	*Interface*	*Commentaire*
127.0.0.0	127.0.0.1	Loopback	*Remise directe*
193.12.5.0	193.12.5.21	LAN Ethernet	*Remise directe*

- **EXPRESSION des CAS de « REMISE INDIRECTE » :**

Deux techniques :

☞***Routage par saut successif :***

☞***Routage par défaut :***

ROUTAGE IP (4/7) : TECHNIQUES (2/3)

- **ROUTAGE par SAUTS SUCCESSIFS :**

Principe :

☞***Dans ce cas :***

@sse IP de réseau : représente l'adresse IP d'un réseau destinataire,

@sse IP de routeur : représente l'adresse IP du routeur suivant sur le chemin qui mène au réseau destinataire et accessible directement par la liaison associée à interface.

☞***Une telle entrée n'indique qu'une étape (un « hop ») sur le chemin qui mène au réseau cible : il s'agit du « saut suivant » à effectuer.***

☞***Les routeurs dont les adresses apparaissent dans une telle table de routage sont directement accessibles sur un réseau donné.***

Illustration :

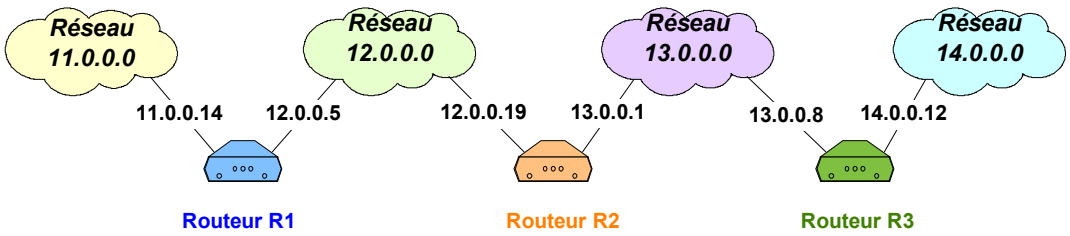


Table de routage de R2 :

Réseau destinataire	*Décision routage*	*Commentaire*
12.0.0.0	12.0.0.19	*Remise directe*
13.0.0.0	13.0.0.1	*Remise directe*
11.0.0.0	12.0.0.5	*Via R1*
14.0.0.0	13.0.0.8	*Via R3*

Table de routage de R3 :

Réseau destinataire	*Décision routage*	*Commentaire*
14.0.0.0	14.0.0.12	*Remise directe*
13.0.0.0	13.0.0.8	*Remise directe*
11.0.0.0	13.0.0.1	*Via R2*
12.0.0.0	13.0.0.1	*Via R2*

ROUTAGE IP (5/7) : TECHNIQUES (3/3)

- **ROUTAGE par DÉFAUT :**

Principe :

☞*Une seule entrée de la table de routage est de la forme :*

(default, @sse IP de routeur)

où :

default *: permet de traiter toutes les adresses de destination qui ne sont pas mentionnées précédemment dans la table de routage,*

@sse IP de routeur *: représente l'adresse IP du routeur à qui expédier, via interface, un datagramme à destination de l'une de ces adresses non mentionnées.*

☞*Cette technique qui consiste à prévoir un routeur par défaut allège considérablement les tables de routage.*

Illustration :

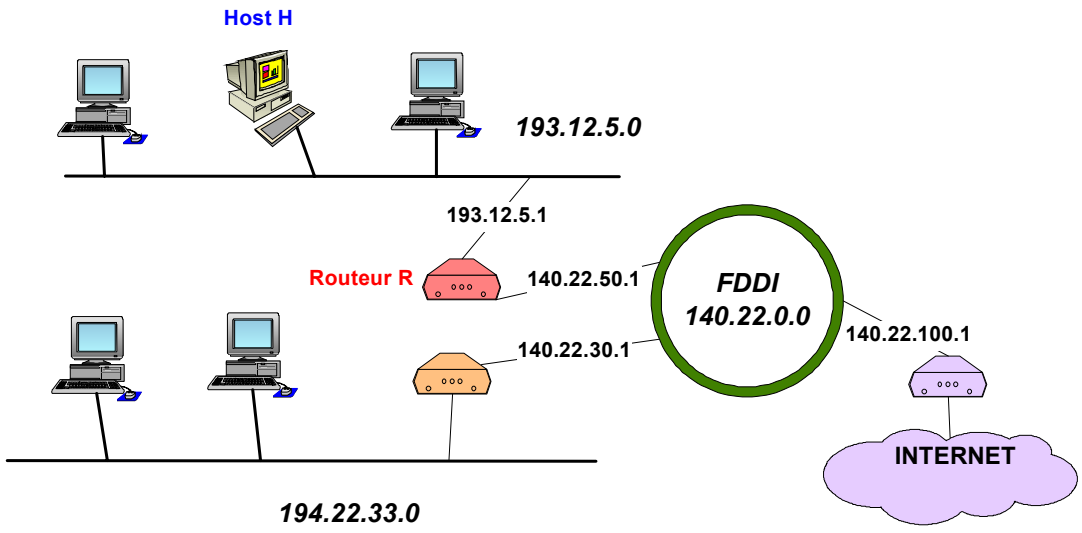


Table de Routage de R

Réseau destinataire	*Décision routage*
140.22.0.0	140.22.50.1
193.12.5.0	193.12.5.1
194.22.33.0	140.22.30.1
default	140.22.100.1

Table de Routage sur H

Réseau destinataire	*Décision routage*
193.12.5.0	193.12.5.21
default	193.12.5.1

ROUTAGE IP (6/7) : POLITIQUES (1/1)

- **POLITIQUES de ROUTAGE :**

Mode de constitution des tables de routage, deux techniques :

- **Routage STATIQUE :**

☞Routage déterminé a priori, tables entrées manuellement par l'administrateur.

☞Commandes système : route

- **Routage DYNAMIQUE :**

☞Calculer et déterminer dynamiquement les tables de routage : adaptation à l'état courant du réseau (topologie, charge, …) et optimisation des routes (plus court chemin)

- **PRINCIPE d'un ROUTAGE DYNAMIQUE :**

☞Algorithme distribué : chaque routeur applique le même algorithme pour déterminer les tables de routage.

☞Protocoles de routage : supports de l'échange d'informations de routage entre routeurs voisins.

☞Deux grandes techniques de base :

- **ROUTAGE par VECTEURS DISTANCE :**

☞Chaque noeud conserve la valeur de la distance entre lui-même et chaque destination possible : c'est le vecteur distance. Ce vecteur distance est calculé à partir des vecteurs distances des noeuds voisins.

☞Cette technique est directement issue des algorithmes de Bellman et de Ford (version distribuée).

☞RIP, RIP2 (Intra Domaine), EGP, BGP (Inter Domaine).

- **ROUTAGE par ETATS de LIAISONS :**

☞Chaque noeud construit et maintient une copie complète de la carte du réseau et calculent localement les meilleurs chemins par l'algorithme de Dijsktra.

☞Les modifications de topologie sont communiquées aux autres noeuds par un algorithme d'inondation sélective.

☞OSPF (Intra Domaine), IDPR (Inter Domaine).

ROUTAGE IP (7/7) : ALGORITHME de PRISE de DECISION

- **ALGORITHME UNIFIÉ :**

Valable pour un Host et un Routeur :

```
Choisir_Route_Datagramme_IP(Datagramme, Table_de_Routage)

  DEBUT

    Extraire l'adresse IP de destination, D, du datagramme ;

    Calculer l'identificateur du réseau de destination, N ;

    SI N correspond à une adresse de réseau directement accessible
    ALORS
        Envoyer le datagramme vers la destination D, sur ce
        réseau ;
        /* Cela revient à effectuer une résolution d'adresse, à
        l'encapsulation du datagramme et à la transmission de la
        trame */
    SINON
      SI la table de routage indique que D correspond à un routage
      de Host à Host
      ALORS
        Transmettre vers le saut suivant précisé dans la table de
        routage ;
      SINON
        SI la table de routage contient une route pour le réseau N
        ALORS
          Transmettre le datagramme vers le saut suivant précisé
          par la table de routage ;
        SINON
          SI il existe une route par défaut
          ALORS
            Transmettre le datagramme vers le routeur par défaut
            précisé dans la table de routage ;
          SINON
            Déclarer une erreur de routage ;
  FIN
```

Synthèse IP (1/2) : Les PRIMITIVES de SERVICE

Un utilisateur du service IP dispose de l'équivalent de deux primitives de service :

- ***une primitive de demande d'émission (~ N-UNIT-DATA.REQ)***
- ***une primitive d'indication de réception (~ N-UNIT-DATA.IND)***

- **PRIMITIVE d'ÉMISSION :**
  - **Paramètres fournis par l'utilisateur de service :**
    - **adresses IP source et destinataire,**
    - **numéro du protocole utilisateur,**
    - **services souhaités,**
    - **identificateur du paquet,**
    - **autorisation ou non de fragmentation,**
    - **durée de vie initiale,**
    - **longueur des données à émettre,**
    - **options,**
    - **données.**

- **PRIMITIVE de RÉCEPTION :**
  - **Paramètres fournis à l'utilisateur de service :**
    - **adresses IP source et destinataire,**
    - **numéro du protocole utilisateur,**
    - **indicateurs de types de service,**
    - **longueur des données reçues,**
    - **options,**
    - **données reçues.**

Synthèse IP (2/2) : Les OPÉRATIONS du PROTOCOLE

Suivant la nature de l'équipement où il est implanté, le logiciel IP réalise des opérations pour mettre en oeuvre le protocole IP et rendre le service IP attendu :

- **Sur un HOST :**
  - **Lors de l'ÉMISSION :**

    ☞ *Construire un datagramme sur la base des paramètres de la primitive de service EMISSION,*

    ☞ *Calculer le checksum et l'inclure dans l'en-tête du datagramme,*

    ☞ *Prendre une décision de routage selon l'algorithme unifié (Une résolution d'adresse peut être alors exécutée),*

    ☞ *Transmettre le datagramme à l'interface réseau.*

  - **Lors de la RÉCEPTION :**

    ☞ *Si l'adresse destinataire ne correspond pas, détruire le datagramme,*

    ☞ *Vérifier le checksum, si erreur détruire le datagramme,*

    ☞ *Si nécessaire et possible, effectuer le réassemblage,*

    ☞ *Transmettre, à partir de l'en-tête et des données, à l'utilisateur les paramètres de la primitive de service INDICATION de RECEPTION.*

- **Sur un ROUTEUR :**
  - **Dans le cas où le routeur n'est pas la destination finale :**

    ☞ *Vérifier le checksum, si erreur détruire le datagramme,*

    ☞ *Décrémenter la durée de vie, si elle devient nulle détruire le datagramme,*

    ☞ *Prendre une décision de routage selon l'algorithme unifié,*

    ☞ *Si nécessaire, fragmenter le datagramme,*

    ☞ *Pour chaque datagramme à expédier :*
    - *Reconstruire le nouvel en-tête*
    - *Transmettre à l'interface réseau.*

    GÉNÉRER un MESSAGE ICMP approprié si NÉCESSAIRE !